CLAIMS:

What is claimed is:

1. A method for providing secure access to console functions of a computer system comprising:

initiating a first EKE sequence to generate a device shared secret utilizing a default device identifier and associated shared secret on a system-attached device from which a console operation is desired enabled;

generating said device shared secret from said first EKE sequence, wherein said device shared secret is utilized in place of said default device shared secret in subsequent console authentication procedures; and

storing said device shared secret within a storage location of said system and on said system-attached device.

2. The method of Claim 1, wherein said shared secret is stored in a protected manner on said system-attached device and utilized with a device ID during each connection of said system-attached device to said system.

3. The method of Claim 2, further comprising encrypting operator authentication data flowing between said system-attached device and said system utilizing said shared secret.

4. The method of Claim 2, method further comprising encrypting operator authentication data flowing between said system-attached device and said system utilizing a hash of said shared secret.

5. The method of Claim 2, further comprising:

responsive to an establishment of a first console session that authenticates said system-attached device, instantiating a second EKE sequence to authenticate a console operator utilizing a default user identifier and password; and

storing said user identifier and password in a protected area of said storage location of said system.

6. The method of Claim 5, further comprising:

enabling a setup of multiple device identifiers and authorization levels for other system-attached devices to act as console devices; and

storing said multiple device identifiers and authorization levels in said storage location.

7. The method of Claim 5, further comprising:

enabling a setup of multiple operator user identifiers and associated passwords and authorization levels for other console operators to access console functions of the system; and

storing said multiple operator user identifiers and associated passwords and authorization levels in said storage location.

8. The method of Claim 5, further comprising enabling multiple console sessions for different systems on a single console device.

9. A system for providing secure access to console functions of a computer system comprising logic for:

initiating a first EKE sequence to generate a device shared secret utilizing a default device identifier and associated shared secret on a system-attached device from which a console operation is desired enabled;

generating said device shared secret from said first EKE sequence, wherein said device shared secret is utilized in place of said default device shared secret in subsequent console authentication procedures; and

storing said device shared secret within a storage location of said system and on said system-attached device.

10. The system of Claim 9, wherein said shared secret key is stored in a protected manner on said system-attached device and utilized as a device ID during each connection of said system-attached device to said system.

11. The system of Claim 10, further comprising encrypting operator authentication data flowing between said system-attached device and said system utilizing said shared secret.

12. The system of Claim 10, method further comprising logic for encrypting operator authentication data flowing between said system-attached device and said system utilizing a hash of said shared secret.

13. The system of Claim 10, further comprising logic for:

responsive to an establishment of a first console session that authenticates said system-attached device, instantiating a second EKE sequence to authenticate a console operator utilizing a default user identifier and password; and

storing said user identifier and password in a protected area of said storage location of said system.

14. The system of Claim 13, further comprising logic for:

enabling a setup of multiple device identifiers and authorization levels for other system-attached devices to act as console devices; and

storing said multiple device identifiers and authorization levels in said storage location.

15. The system of Claim 13, further comprising logic for:

enabling a setup of multiple operator user identifiers and associated passwords and authorization levels for other console operators to access console functions of the system; and

storing said multiple operator user identifiers and associated passwords and authorization levels in said storage location.

16. The system of Claim 13, further comprising logic for enabling multiple console sessions for different systems on a single console device.

17. A computer program product comprising:

a computer readable medium; and

program code on said computer readable medium for providing secure access to console functions of a computer system by:

initiating a first EKE sequence to generate a device shared secret utilizing a default device identifier and associated shared secret on a system-attached device from which a console operation is desired enabled;

generating a device shared secret from said first EKE sequence, wherein said device shared secret is utilized in place of said default device shared secret in subsequent console authentication procedures; and

storing said device shared secret within a storage location of said system and on said system-attached device.

18. The computer program product of Claim 17, wherein said shared secret key is stored in a protected manner on said system-attached device and utilized as a device ID during each connection of said system-attached device to said system.

19. The computer program product of Claim 18, further comprising program code for encrypting operator authentication data flowing between said system-attached device and said system utilizing said shared secret.

20. The computer program product of Claim 18, further comprising program code for encrypting operator authentication data flowing between said system-attached device and said system utilizing a hash of said shared secret.

21. The computer program product of Claim 18, further comprising program code for:

responsive to an establishment of a first console session that authenticates said system-attached device, instantiating a second EKE sequence to authenticate a console operator utilizing a default user identifier and password; and

storing said user identifier and password in a protected area of said storage location of said system.

22. The computer program product of Claim 21, further comprising program code for:

enabling a setup of multiple device identifiers and authorization levels for other system-attached devices to act as console devices; and

storing said multiple device identifiers and authorization levels in said storage location.

23. The computer program product of Claim 21, further comprising program code for:

enabling a setup of multiple operator user identifiers and associated passwords and authorization levels for other console operators to access console functions of the system; and

storing said multiple operator user identifiers and associated passwords and authorization levels in said storage location.

24. The computer program product of Claim 21, further comprising program code for enabling multiple console sessions for different systems on a single console device.

25. A method of signing in authenticated users to a console function of a system, comprising:

determining via a first EKE sequence whether a device identifier and associated shared secret of a system-attached device matches a stored device identifier and associated shared secret on said system;

responsive to both ends having identical shared secrets, receiving a user-entered identifier and password;

responsive to said receiving, initiating a second EKE sequence to determine whether said user-entered identifier and password matches a user identifier and password combination stored on a storage location of said system; and

granting said user access to console functions only when said second EKE sequence is successful.

26. The method of Claim 25, further comprising encrypting data transmitted during said second EKE sequence utilizing a shared secret generated during said first EKE sequence.

27. A method for secure authentication of a system console device within a network environment, comprising:

establishing a first console session from an authentication device, wherein a default device identifier is utilized to initiate an EKE sequence between a network-attached console device and a..

generating a shared secret key via an EKE sequence utilized to establish said first console session; and

subsequently authenticating a console operator via a second EKE sequence, wherein said shared secret key is utilized to encrypt data of an authentication process for said console operator attempting to utilize said console operation.